IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Cain	
Application No.: 09/661,273	Group Art Unit: 2155
Filed: 9/13/2000	Examiner: Nguyen
Title: System, Device & Method for Receiver Access Control in an Internet Television System	
Attorney Docket No.: 120-194 2204/A50	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF PURSUANT TO 37 C.F.R. § 1.192

This Appellant's brief is hereby submitted in accordance with a Notice of Appeal filed with this brief.

I. Real Party in Interest

The real party in interest is Nortel Networks Limited, 380 Antoine Street West, 8th Floor, Montreal, Quebec, H2Y 3Y4, Canada.

II. Related Appeals and Interferences

Appellants are not aware of any appeals or interferences that are related to the present case.

III. Status of the Claims

This is an appeal from an office action dated January 29, 2007, in which claims 1-55 are subject to final rejection. Claims 1-55 are currently pending in the present application. No claims have been allowed. The rejections of claims 1, 15, 25, 35, 45 and 55 are the subject of this appeal. All claims are listed in Appendix A.

IV. Status of Amendments

The most recent Amendment was submitted on November 10, 2006. That Amendment was entered and considered by the Office, as were all previous Amendments.

V. Summary of Claimed Subject Matter

The claimed subject matter concerns access control in an Internet television system. For many years, television signals were almost exclusively delivered via land-based wireless broadcast. The television signals were not encrypted, and anyone with a receiver could view the channel being broadcast. Subscription-based cable and satellite television service has now displaced broadcast television in some regions, although many of the broadcast television channels are still provided over cable and satellite. Cable and satellite systems often require use of a subscriber set-top box to decode and decrypt the incoming television signal. One purpose of the set-top box is to prevent unauthorized viewing of the channels, i.e., by non-subscribers. More recently, the Internet is being considered for delivery of television signals. One proposal for delivering television over the Internet is to use Internet Protocol ("IP") multicasting. In particular, a television channel could be carried by a multicast group, i.e., a unique multicast group would exist for each channel. In order to change channels, the television or set-top box would migrate to a different multicast group. However, it is technically challenging to both exclude non-subscribers from particular multicast groups and permit the speedy channel changes to which subscribers have become accustomed, i.e., to have security and fast group membership changes.

Claim 1 recites an access control method for an internet television system where each television channel is carried over a different multicast group and subscribers join a particular multicast group in order to receive a particular channel. The recited limitation "distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to reduce delay in authentication when a host device changes television channels" is supported in the Specification at page 5, lines 14-21. The limitation "wherein each access device is logically closer to the host device from which the access device receives the request than the distribution device" is supported by Figure 1 and the corresponding description at page 5, lines 26-29. The limitation "receiving, by one of the access devices, a subsequent request by one of the host devices to join the television channel multicast group in order to change television channels" is supported in the Specification at page 9, line 30 through page 10, line 2. The limitation "determining, by the access device, whether the host device is authorized to join the television channel multicast group, and receive a particular television channel, based upon the access control information distributed from the distribution device" is supported in the Specification at page 10, lines 2 through 3. The limitation "admitting, by the access device, the host device to the television channel multicast group if and only if the host device is determined to be authorized to join the television channel multicast group" is supported in the Specification at page 10, lines 3 through 11. The limitation "whereby the access device receives the access control information before it is needed for determining whether the host device is authorized to join the multicast group, thereby facilitating changing channels by reducing authentication delay" is supported in the specification at page 5, lines 14 through 21.

Claim 15 recites an apparatus for distributing access control information in an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device. The limitation "maintenance logic and memory operably coupled to maintain multicast group access control information" is supported in the Specification at page 6, line 26 through page 7, line 3. The limitation "distribution logic and an interface operably coupled to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels," is supported in the Specification at page 7, line 4 through page 8, line 8. The limitation "wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information" is supported by Figure 1 and the corresponding description at page 5, lines 26-29. The limitation "whereby the access device receives the access control information before it is needed for determining whether a host device is authorized to join a multicast group, and receive a particular television channel, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay" is supported in the specification at page 5, lines 14 through 21.

Claim 25 recites a computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device. The limitation “maintenance logic programmed to maintain multicast group access control information” is supported in the Specification at page 6, line 26 through page 7, line 3. The limitation “distribution logic programmed to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels” is supported in the Specification at page 7, line 4 through page 8, line 8. The limitation “wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information” is supported by Figure 1 and the corresponding description at page 5, lines 26-29. The limitation “whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay” is supported in the specification at page 5, lines 14 through 21.

Claim 35 recites an apparatus for providing receiver access control in an internet television system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device. The limitation “distribution logic operably coupled to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels” is supported in the Specification at page 7, line 4 through page 8, line 8. The limitation "host interface logic operably coupled to receive a request from a host device to join a television channel multicast group" is supported in the Specification at page 9, line 30 through page 10, line 2. The limitation "access control logic operably coupled to determine whether the host device is authorized to join the television channel multicast group based upon the access control information" is supported in the Specification at page 10, lines 2 through 3. The limitation "wherein the apparatus is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay" is supported by Figure 1 and the corresponding description at page 5, lines 26-29, and also at page 5, lines 14 through 21.

Claim 45 recites a computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device. The limitation "distribution logic programmed to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels" is supported in the Specification at page 7, line 4 through page 8, line 8. The limitation "host interface logic programmed to receive a request from a host device to join a television channel multicast group" is supported in the Specification at page 9, line 30 through page 10, line 2. The limitation "access control logic programmed to determine whether the host device is authorized to join the television channel multicast group based upon the access control information" is supported in the Specification at page 10, lines 2 through 3. The limitation "wherein the host interface logic is executed by a device that is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay" is supported by Figure 1 and the corresponding description at page 5, lines 26-29, and also at page 5, lines 14 through 21.

Claim 55 recites an internet television system for delivering a video signal to a host device for display. The limitation "a distribution device in communication with at least one access device over a communication network, wherein the distribution device uses a predetermined push mechanism to distribute multicast group access control information to the at least one access device in order to reduce delay in authentication when a host device changes television channels" is supported in the Specification at page 7, line 4 through page 8, line 8. The limitation "wherein the at least one access device uses the access control information to control access to at least one television channel multicast group" is supported in the Specification at page 10, lines 2 through 3. The limitation "wherein the access device is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay" is supported by Figure 1 and the corresponding description at page 5, lines 26-29, and also at page 5, lines 14 through 21.

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 15, 25, 35, 45, and 55 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent 5,748,736 to Mittra ("'736 patent").

Claims 15 and 35 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

VII. Argument

The Rejections Based on §102(b)

35 U.S.C. §102(b) states that a person shall be entitled to a patent unless the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States. It is well established that under §102 "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). Appellants assert that the rejections of claims 1, 15, 25, 35, 45 and 55 under 35 U.S.C. §102 fail to meet this requirement, since

the ‘736 patent does not include the claimed limitation of distributing the **access control information** from the main server to the access devices in such a way that the access devices receive the access control information before it is needed and without requesting or otherwise retrieving the access control information from the main server.

Both the ‘736 patent and the Specification of this application describe a network with a main server, intermediate access devices, and subscriber devices. The ‘736 patent describes the main server as a “group security controller (GSC)”[1], whereas the present application uses the term “distribution server 110.”[2] The ‘736 patent describes the intermediate devices as “trusted intermediary (TI) servers,”[3] whereas the present application uses the term “access device 130.”[4] Finally, the ‘736 patent describes the subscriber devices as “receivers 114,”[5] whereas the present application uses the term “host 140.”[6] Since the Office maintains that these devices are equivalent, it is important that the relationships between these terms are clear:

main server: **GSC** allegedly equivalent to **distribution server**

intermediate device: **TI** allegedly equivalent to **access device**

subscriber device: **receiver** allegedly equivalent to **host**.

[1] Abstract
[2] Page 5, line 27
[3] Abstract
[4] Page 5, line 27
[5] Column 6, lines 3 through 37
[6] Page 5, line 28

The '736 patent describes a technique for joining a secure multicast group which differs significantly from the presently claimed invention. With regard to the role of the TI server, the '736 patent states:

> TI servers are authorized to act as proxies for the GSC. Each TI server can **approve changes in group membership** below it (i.e., it can approve changes in group membership in the sub-group served thereby), thus **isolating the effects of these changes in group membership from the GSC** and the members that are not associated with the TI server approving the change. Thus a **TI server acts as the GSC** for members of "its" multicast group. This **isolation to changes** allows the inventive system to scale well to groups with large memberships and frequent changes in membership.[7]

In other words, the TI server is authorized to add/remove group members without member-specific authorization from the GSC. In contrast with the GSC of the '736 patent, the distribution server of the present invention is not isolated from changes in group membership, and retains control over group membership of the subscriber/hosts. The access control information is moved to the access device in order to be closer to the subscriber/host, and thereby speed membership and channel changes, but the access device does not make membership add/drop decision. Rather, the access device enforces the membership dictated by the distribution server.

The distinguishing limitation discussed above is recited in claim 1 as "distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel

[7] Column 12, line 60 through Column 13, line 3 (emphasis added)

multicast group in order to reduce delay in authentication when a host device changes television channels … determining, by the access device, whether the host device is authorized to join the television channel multicast group, and receive a particular television channel, **based upon the access control information distributed from the distribution device**." (emphasis added). Similarly, claim 15 recites "maintenance logic and memory operably coupled to maintain multicast group access control information; and distribution logic and an interface operably coupled to distribute the access control information to at least one access device … wherein the access device is operable to transmit the channel to the host device … whereby the access device receives the access control information before it is needed for determining whether a host device is authorized to join a multicast group." Claim 25 distinguishes the '736 patent by reciting "distribution logic programmed to distribute the access control information to at least one access device … whereby the access device receives the access control information before it is needed." aim 35 distinguishes the '736 patent by reciting "distribution logic operably coupled to receive multicast group access control information from a distribution device … access control logic operably coupled to determine whether the host device is authorized to join the television channel multicast group based upon the access control information." Claim 45 distinguishes the '736 patent by reciting "distribution logic programmed to receive multicast group access control information from a distribution device … access control logic programmed to determine whether the host device is authorized to join the television channel multicast group based upon the access control information."

Claim 55 distinguishes the '736 patent by reciting "a distribution device in communication with at least one access device over a communication network, wherein the distribution device uses a predetermined push mechanism to distribute multicast group access control information to the at least one access … and wherein the at least one access device uses the access control information to control access to at least one television channel multicast group. The dependent claims, although not the subject of this appeal, are allowable over the '736 patent for the same reasons as their respective base claims.

The Office asserts that the limitation discussed above is taught in the '736 patent at column 3, line 49 through column 13, line 36. However, with the possible exception of one sentence, that passage describes only security through key management. As discussed above, the presently claimed invention is directed to access control, rather than encryption and key management. Further, providing a decryption key to a subscriber does not make the subscriber a member of a multicast group. At column 4, lines 11 through 14, it is stated that "the GSC and each TI server are responsible for maintaining the security of the group by authenticating and authorizing all members of the multicast." However, as already discussed above with reference to Column 12, line 60 through Column 13, line 3, the responsibility of the TI server in authorization includes making independent decisions about adding members to the multicast group, whereas the presently claimed access device does not make independent decisions, but rather remains under the control of the server.

It should be noted that in addition to differing from the presently claimed invention in terms of joining a multicast group, the teaching of the ‘736 patent also differs in providing security. In order to provide secure multicast, the ‘736 patent teaches that “in each embodiment of the inventive system, the secure multicast group has a hierarchical structure … with each of the sub-groups being served by a different TI server,”[8] where “the overall secure multicast group does not employ a single, common group key,”[9] but rather “each TI server multicasts data to the members of its subgroup using its own group key.”[10] In other words, the ‘736 patent teaches that security is provided by encryption. In contrast with the ‘736 patent, the presently claimed invention recites that the access device performs access control based on group membership information obtained beforehand from the distribution device. As a result, access control, rather than encryption, provides security against unauthorized access by non-subscribers. Each of the independent claims 1, 15, 25, 35, 45, and 55 therefore distinguish the ‘736 patent by reciting that multicast group access control information is distributed from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group.

[8] Column 6, line 67 through column 7, line 3
[9] Column 7, lines 8 through 9
[10] Column 7, lines 9 through 11

The Rejections Based on §101

35 U.S.C. §101 states that whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The Office asserts that claim 15, as recently amended, lacks support in the Specification and Drawings for the recited memory and interface. With regard to the interface, support is in the Specification at page 6, lines 28 through 30, which describes a management interface, and in Figure 4, which illustrates "host interface logic 408." With regard to the memory, support is in the Specification at page 6, line 26, which describes the access control information as being maintained in a database. Figure 2, step (204) similarly describes maintaining access control information. Applicant assert that there is no other practical means for storage of such information than a memory, and that this is understood by those of ordinary skill in the art.

With regard to claims 15 and 35, the Office asserts that it is unclear how a logic/program can couple to a memory. Applicant's understanding is that such a coupling is typically accomplished via Read and Write operations, and may utilize pointers to specific locations, all of which is well understood by those of ordinary skill in the art. Applicant is aware that the Office has recently issued Interim Guidelines which, in effect, require the recitation of particular language on the grounds that the language renders computer programs statutory. However, claims 15 and 35 are apparatus claims, rather than computer program claims. In both claims, the preamble recites “An apparatus for providing receiver access control in an internet television system.” Further, just because the logic may be partitioned into the recited logic blocks, it does not follow that the logic blocks are abstract software, and Applicant acknowledges and states for the record that the recited logic is embodied in something tangible. Note that claims 25 and 45 specifically recite computer programs.

VIII. Conclusion

Appellants submit that the rejections of claims 1, 15, 25, 35, 45, and 55 under 35 U.S.C. §102, and the rejections of claims 15 and 35 under 35 U.S.C. §101, are improper for at least the reasons set forth above. Appellants accordingly request that the rejections be withdrawn and the application put forward for allowance.

Respectfully submitted,

NORTEL NETWORKS LTD.

By: /Holmes W. Anderson/

Holmes W. Anderson
Reg. No. 37,272
Attorney for Assignee

Date: March 28, 2007

McGuinness & Manaras LLP
125 Nagog Park
Acton MA 01720
(978) 264-4001

Appendix A - Claims

1. (previously presented) An access control method for an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel, the access control method comprising:

distributing multicast group access control information from a distribution device to a plurality of access devices for use by the access devices in authenticating subsequent requests by individual host devices to join a television channel multicast group in order to reduce delay in authentication when a host device changes television channels, wherein each access device is logically closer to the host device from which the access device receives the request than the distribution device;

receiving, by one of the access devices, a subsequent request by one of the host devices to join the television channel multicast group in order to change television channels;

determining, by the access device, whether the host device is authorized to join the television channel multicast group, and receive a particular television channel, based upon the access control information distributed from the distribution device; and

admitting, by the access device, the host device to the television channel multicast group if and only if the host device is determined to be authorized to join the television channel multicast group, whereby the access device receives the access control information before it is needed for determining whether the host device is authorized to join the multicast group, thereby facilitating changing channels by reducing authentication delay.

2. (original) The access control method of claim 1, wherein distributing the access control information from the distribution device to the access device comprises:

pushing the access control information from the distribution device to the access control device using a predetermined push mechanism.

3. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

4. (original) The access control method of claim 3, wherein pushing the access control information from the distribution device to the access control device using the predetermined push mechanism comprises:

joining a predetermined multicast group by the access device;

sending the access control information to the predetermined multicast group by the distribution device using the reliable multicast mechanism;

receiving the access control information by the access device from the multicast group using the reliable multicast mechanism.

5. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a policy service.

6. (original) The access control method of claim 5, wherein the policy service comprises a Common Open Policy Service (COPS).

7. (original) The access control method of claim 5, wherein pushing the access control information from the distribution device to the access control device using a predetermined push mechanism comprises:

sending the access control information from the distribution device to the access device in the form of policy information using the policy service.

8. (original) The access control method of claim 2, wherein the predetermined push mechanism comprises a management mechanism.

9. (original) The access control method of claim 8, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

10. (original) The access control method of claim 8, wherein the management mechanism comprises a Command Line Interface (CU).

11. (original) The access control method of claim 8, wherein pushing the access control information from the distribution device to the access control device using a predetermined push mechanism comprises:

sending the access control information from the distribution device to the access device in the form of management information using the management mechanism.

12. (original) The access control method of claim 1, wherein determining whether the host device is authorized to join the television channel multicast group comprises:

authenticating the host device based upon the access control information.

13. (original) The access control method of claim 1, wherein admitting the host device to the television channel multicast group comprises:

joining the television channel multicast group by the access device using a predetermined multicast routing protocol.

14. (original) The access control method of claim 13, wherein the predetermined multicast routing protocol comprises a Protocol Independent Multicast (PIM) multicast routing -protocol.

15. (previously presented) An apparatus for distributing access control information in an internet television system where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

maintenance logic and memory operably coupled to maintain multicast group access control information; and distribution logic and an interface operably coupled to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels, wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information,

whereby the access device receives the access control information before it is needed for determining whether a host device is authorized to join a multicast group, and receive a particular television channel, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

16. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

17. (original) The apparatus of claim 16, wherein the distribution logic is operably coupled to send the access control information to a predetermined multicast group using the reliable multicast mechanism.

18. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a policy service.

19. (original) The apparatus of claim 18, wherein the policy service comprises a Common Open Policy Service (COPS).

20. (original) The apparatus of claim 18, wherein the distribution logic is operably coupled to send the access control information to the access device in the form of policy information using the policy service.

21. (original) The apparatus of claim 15, wherein the predetermined push mechanism comprises a management mechanism.

22. (original) The apparatus of claim 21, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

23. (original) The apparatus of claim 21, wherein the management mechanism comprises a Command Line Interface (CLI).

24. (original) The apparatus of claim 21, wherein the distribution logic is operably coupled to send the access control information from the distribution device to the access device in the form of management information using the management mechanism.

25. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast

group in order to receive a particular channel at a host device, the computer program comprising:

maintenance logic programmed to maintain multicast group access control information; and

distribution logic programmed to distribute the access control information to at least one access device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels, wherein the access device is operable to transmit the channel to the host device and is logically closer to the host device than the apparatus for distributing access control information,

> whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

26. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

27. (original) The computer program of claim 26, wherein the distribution logic is programmed to send the access control information to a predetermined multicast group using the reliable multicast mechanism.

28. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a policy service.

29. (original) The computer program of claim 28, wherein the policy service comprises a Common Open Policy Service (COPS).

30. (original) The computer program of claim 28, wherein the distribution logic is programmed to send the access control information to the access device in the form of policy information using the policy service.

31. (original) The computer program of claim 25, wherein the predetermined push mechanism comprises a management mechanism.

32. (original) The computer program of claim 31, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

33. (original) The computer program of claim 31, wherein the management mechanism comprises a Command Line Interface (CLI).

34. (original) The computer program of claim 31, wherein the distribution logic is programmed to send the access control information from the distribution device to the access device in the form of management information using the management mechanism.

35. (previously presented) An apparatus for providing receiver access control in an internet television system for delivering television where each television channel is

carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the apparatus comprising:

distribution logic operably coupled to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

host interface logic operably coupled to receive a request from a host device to join a television channel multicast group; and

access control logic operably coupled to determine whether the host device is authorized to join the television channel multicast group based upon the access control information, wherein the apparatus is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

36. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

37. (original) The apparatus of claim 36, wherein the distribution logic is operably coupled to join a predetermined multicast group and receive the access control information from the predetermined multicast group using the reliable multicast mechanism.

38. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises a policy service.

39. (original) The apparatus of claim 38, wherein the policy service comprises a Common Open Policy Service (COPS).

40. (original) The apparatus of claim 38, wherein the distribution logic is operably coupled to receive the access control information from the distribution device in the form of policy information using the policy service.

^

41. (original) The apparatus of claim 35, wherein the predetermined push mechanism comprises

a management mechanism.

42. (original) The apparatus of claim 41, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

43. (original) The apparatus of claim 41, wherein the management mechanism comprises a Command Line Interface (CLI).

44. (original) The apparatus of claim 41, wherein the distribution logic is operably coupled to receive the access control information from the distribution device in the form of management information using the management mechanism.

45. (previously presented) A computer program embedded in a tangible storage medium for controlling a computer system for delivering television where each television channel is carried over a different multicast group, and subscribers join a particular multicast group in order to receive a particular channel at a host device, the computer program comprising:

distribution logic programmed to receive multicast group access control information from a distribution device using a predetermined push mechanism in order to reduce delay in authentication when a host device changes television channels;

host interface logic programmed to receive a request from a host device to join a television channel multicast group; and

access control logic programmed to determine whether the host device is authorized to join the television channel multicast group based upon the access control information, wherein the host interface logic is executed by a device that is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

46. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a reliable multicast mechanism.

47. (original) The computer program of claim 46, wherein the distribution logic is programmed to join a predetermined multicast group and receive the access control information from the predetermined multicast group using the reliable multicast mechanism.

48. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a policy service.

49. (original) The computer program of claim 48, wherein the policy service comprises a Common Open Policy Service (COPS).

50. (original) The computer program of claim 48, wherein the distribution logic is programmed to receive the access control information from the distribution device in the form of policy information using the policy service.

51. (original) The computer program of claim 45, wherein the predetermined push mechanism comprises a management mechanism.

52. (original) The computer program of claim 51, wherein the management mechanism comprises a Simple Network Management Protocol (SNMP).

53. (original) The computer program of claim 51, wherein the management mechanism comprises a Command Line Interface (CU).

54. (original) The computer program of claim 51, wherein the distribution logic is programmed to receive the access control information from the distribution device in the form of management information using the management mechanism.

55. (previously presented) An internet television system for delivering a video signal to a host device for display, comprising:

a distribution device in communication with at least one access device over a communication network, wherein the distribution device uses a predetermined push mechanism to distribute multicast group access control information to the at least one access device in order to reduce delay in authentication when a host device changes television channels, and wherein the at least one access device uses the access control information to control access to at least one television channel multicast group, wherein the access device is logically closer to the host device than the distribution device, whereby the access device receives the access control information before it is needed, and whereby access control information is moved closer to the host device, thereby facilitating changing channels by reducing authentication delay.

Appendix B - Evidence Submitted

None.

Appendix C - Related Proceedings

None.